www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

AI-Powered Individualized Cybersecurity Education and Awareness

[1]Mr. Ch Surya Prakash, [2] Jaddu Keerthi Sai,

[1]Associate Professor, Department of MCA, Rajamahendri Institute of Engineering & Technology. Bhoopalapatnam, Near Pidimgoyyi,Rajahmundry,E.G.Dist.A.P. 533107.

[2]Student,Department of MCA, RajamahendriInstitute of Engineering & Technology. Bhoopalapatnam, Near Pidimgoyyi,Rajahmundry,E.G.Dist.A.P. 533107.

Abstract—

Cyber security has made good use of artificial intelligence (AI) to better understand, investigate, and assess cyber dangers. More efficiently, it can foresee cyber threats. AI also aids in the implementation of plans to secure data and assets. Understanding cybersecurity controls and implementing the necessary cyber training and security policies and strategies has proven challenging due to the complexity and ongoing growth of these controls. Lionfish Cyber Security, Ottawa, Canada, Research & Development by Zeina Bitar These recently released criteria are one of several aspects that should be considered while updating, maintaining, and enforcing compliance with Zeinajb@hotmail.com. Artificial intelligence (AI) in cybersecurity has the potential to be an essential tool for raising awareness and educating cyber professionals and academics alike about the need of having a thorough understanding of cybersecurity regulations. This research aims to boost the complete cyber security education life cycle by demonstrating how AI may aid in cybersecurity education and awareness as well as the creation of policies quickly and at the required level. The emphasis is on the efficiency of AI-driven processes.

Keywords— Cyber Security Awareness, Cyber Security Education, AI-driven, Cyber Security Compliance.

INTRODUCTION

The learners' knowledge of cybersecurity during the education life cycle, as well as their interest in receiving training in this domain, can be enhanced using AI-driven mechanisms [1]. Shaw et al. defined cybersecurity education as: ‘‘the degree of understanding of users about the importance of information security and their responsibilities and acts to exercise sufficient levels of information security control to protect the organization’s data and networks’’ [2]. This definition highlights the significance of information security, its associated obligations, and its aim which is to understand and use information security control procedures at the sufficient level to safeguard the information. A survey conducted by the Yobe State University Department of Computer Science found that although the students were aware of cybersecurity, they were unsure of how to safeguard their data [3]. The gap between education and implementation is clear and requires additional actions to ensure efficient implementation of cyber security education. The National Institute of Standards and Technology (NIST), the Cybersecurity Maturity Model Certification (CMMC) [4], and the International Organization for Standardization (ISO) [5] periodically publish new controls and practices to keep up with the industry's best practices. Therefore, cyber security awareness 979-8-3503-8185-6/24/$31.00 ©2024 IEEE Additionally, cybersecurity is developing constantly. Regulatory changes and technological advancements are only two examples of the many elements that contribute to the dynamic and ever-changing nature of the cybersecurity profession. The field of cybersecurity research is always exploring new areas and creating fresh forms of defense. All this makes the generation of new curriculums and higher education content a must. The use of Artificial Intelligence AI in general and ChatGPT in particular, in higher education present many opportunities for the education context that emerge from the release of new AI models [7]. AI models are capable of processing multiple sources of data simultaneously and productively. This makes it possible to rapidly create cybersecurity training materials and resources. AI integration in education can be implemented in various domains. It can help in generating course content, handouts, and lab

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

materials in a customized and personalized way to ensure high efficiency and suitability. This will also help in the practical implementation of newly published regulatory changes for both academic and business needs

CYBERSECURITY EDUCATION AND AWARENESS

A. Raising awareness and educating about cybersecurity Educating the public and potential employers about cyber risks and how to protect themselves and their businesses from them is the goal of cyber security awareness and education programs. This is accomplished by having a firm grasp of cybersecurity fundamentals and by making available training programs, seminars, courses, and resources that deepen this knowledge and equip participants to use best practices in the face of emerging threats. The most common cyber dangers, such as phishing, malware, and social engineering, may be better understood via the implementation of cybersecurity education and awareness programs. Additionally, it provides instructions on how to identify and counteract these dangers.
Also, businesses and people may benefit from incident response training in order to be better prepared to deal with cyber events. Training on how to recognize security breaches and react appropriately to them helps accomplish this goal. Cyber security plans and policies [2][8] implemented by various companies may aid in cataloguing potential risks to resources and offering rules and laws to safeguard both the company and its resources. Employees and suppliers are required to complete awareness training, which forms the basis for some of these requirements. B. Online safety is an ever-evolving field When it comes to cybersecurity, changes are constants. There is growing demand on universities to adequately train their students in cybersecurity as the public becomes more aware of the risks posed by this area. The other side is that cybercriminals are becoming better at what they do. Additionally, there are new methods and resources to circumvent security protocols. Furthermore, there is a constant stream of published updates to existing cybersecurity legislation and standards. Keeping up with the latest developments and defensive techniques is crucial for effective continual learning and adaptation via awareness and education. C. Online research facilities and simulations Cyber security education in the classroom is changing from a focus on rote memorization to more interactive, problem-solving exercises that help students build resilience and knowledge applicable to real-world scenarios [6]. Learners need to be adept in analyzing, understanding, and taking convenient actions in a range of dynamic and perhaps new situations so they can practice incident identification, prevention, and recovery. Labs, both physical and virtual, provide students opportunities to work with real equipment and techniques. These laboratories connect the dots between classroom instruction and official requirements. D. The need for cyber security policy and education for companies An organization's information security rules may be effectively implemented via cyber security awareness and policies [8]. [9]. Organizations continue to experience security breaches despite early budget allocation for compliance and security and the purchase of network security equipment. According to research, social engineering assaults continue to be the leading cause of these security breaches. Raising awareness and providing training may thwart these social engineering attempts. Data theft and other forms of damage may be lessened with well-designed procedures that limit the likelihood of unlawful access to assets and data. It is not easy to evaluate threats, which is another major obstacle in the field of cyber security. Security awareness and well-crafted policies aid in the detection of such risks and provide a framework for the execution of actions that enable businesses to successfully manage them. Fewer cyber risks will result from well implemented awareness strategies, and businesses will be better prepared to respond to triggered threats if their rules are clear. Prior to and after a security trigger, specific steps will be included in the plan. Section E. Recently released cyber security frameworks Organizations may benefit from security frameworks, which are standardized sets of guidelines, standards, laws, and controls for establishing and maintaining reliable cybersecurity programs. To make sure these businesses are up-to-date on best practices, several governments need certification before they would sign contracts with them. As knowledge about effective cybersecurity procedures and standards grows, frameworks are regularly updated to include these best practices and strengthen the overall security posture of businesses. Section F. Frameworks Created by ISO. One prominent group that provides comprehensive documented framework recommendations to aid with data protection is the International Organization for Standardization (ISO). Policies and procedures may be constructed upon these standards, which are arranged in the form of controls. Both ISO 27001 and ISO 2702 are among the most popular guidelines for

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

managing information security. Asset management, access control, incident response, and business continuity are just a few areas that these ISO standards cover in detail to assist organizations with network security [5]. The IT and security departments might also benefit from its assistance in keeping the workplace secure. Next, we have the NIST frameworks. In order to help businesses identify and prevent cyber vulnerabilities and protect their digital assets from cyber-attacks, the US federal organization known as the National Institute of Standards and Technology (NIST) [10] regularly creates and releases normative recommendations and standards. Although the National Institute of Standards and Technology (NIST) frameworks were initially developed with government organizations in mind, many private companies have used them to guarantee the safety of their surroundings and conformity with federal rules. When developing their security strategies, many small and medium-sized enterprises use NIST 800-171, one of many popular NIST frameworks. Protecting Controlled Unclassified Information (CUI) in systems and organizations that are not part of the federal government is outlined in this document. Of the fourteen categories that make up NIST 800 171, the two most important are the Incident Response (IR) and the Access Control (AC) domains. These two areas need stringent supervision since they include the core functions of cyber security operation teams. The National Institute of Standards and Technology (NIST) AI Risk Management Framework exists. The variety of these dangers makes AI implementation challenging. As a result, we need to do more to prevent certain hazards and lessen the impact of the others. To aid companies and people in efficiently and effectively handling AI-related risks

A new AI risk management framework, the AI RMF, was released by NIST not long ago [10]. This framework provides a list of particular dangers linked to the use of AI systems. Chapter Three: AI-Based Cybersecurity Awareness I. Purpose. Various AI systems provide Application Programming Interfaces (APIs) [11] [12] so that other fields may integrate AI capabilities. The application programming interfaces (APIs) provide a framework for automatically communicating with AI models via scripts. Various modules will be able to use AI capabilities as a result of this. Cybersecurity education and awareness may benefit from AI's ability to generate subject- and audience-specific training and instructional materials. The built application that implements the proposed strategy takes two datasets as inputs and produces training and awareness materials as needed. One dataset describes the course (the control) that will be used to create training, while the other includes basic information about the learner (or learning group) (level, background, skill set, etc.). In this approach, the necessary resources and the produced content may be adjusted according to the student's degree of proficiency. After that, the software will create an extensive library of learning items that the user may use to build their own cyber security awareness and training program. Possible evaluations, tasks, and produced rules and procedures will be part of the produced content, which will also include a synopsis, detailed explanation, supplementary materials, and an actionable toolbox with steps. If the needed level isn't reached, the content may be extended and recreated to suit the needs of both the student and the material. Section B. Methods. This newly-developed module generates standardized course materials by specifying the fields for the input and output datasets. Furthermore, it details the necessary input settings for the AI programmable interface to receive the learner's profile, which consists of many non-sensitive data fields. The created module also details the items and controls that the made-up lesson plans need to have easy access to. In addition to the required timeline, it also provides a list of activities that may be used to describe their execution in later stages of schooling. Profile of the learner (C). An important consideration when developing AI-powered instructional materials is the learner profile. For the produced material to be appropriately tailored to the desired profile and to provide the essential effective recommendations, it is vital to utilize the learner-specific profile, goals, and environment. The learner should be able to enter a set of settings into these tools, and the tools should dynamically rely on those values. The necessary dataset is structured into many important fields and provides the foundation for the data used in the created module. Its input parameters have been specified for this context: Networking, routing, switching, firewall setups, cloud architecture, databases, and web applications are just a few of the many technological domains in which expertise is required. One's familiarity with Windows, Linux, and macOS, among others, is a measure of operating system expertise. Both basic and advanced administrative activities should be within one's skill set. • Familiarity with cyber security technologies, such as those used for scanning for vulnerabilities, investigating incidents, and conducting penetration tests. Gaining practical experience is crucial for skill development. This may be achieved via virtual laboratories, physical labs, and real-world initiatives. Compliance in several sectors necessitates familiarity

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

with relevant regulatory frameworks and legislation, such as NIST, GDPR, HIPAA, and PCI-DSS. To succeed in ethical hacking and penetration testing, you must master both offensive and defensive security measures. • The examination and investigation of security events and cybercrime benefits from the competence of digital forensics. The produced instructional material is highly dependent on the user's level of technical competence and familiarity with the operating system. People who are already familiar with Unix, for instance, would rather study and practice with the created content on their preferred OS. Students are more likely to spend more time practicing and ultimately learn more when they are at ease in the setting where they can do so, according to research. Section D. Content Synthesis. The structure of the produced training materials may vary according to the input parameters associated with the learner profile; yet, some core modules should consistently be included. The following is an inventory of all mandatory elements that must be included in the final training documents: • The training's purpose: this section lays forth the overarching aims and primary purposes of the program. • Articles that go into great detail on all the relevant ideas, procedures, and subjects. Because of their adaptability, they serve as main learning materials in conventional classrooms. • Real-world practice is provided via interactive labs and cyber ranges. Students are able to acquire new abilities with their assistance since they provide

students to put their classroom learning into practice. • Practice exams, such as quizzes and mock exams, are great ways to see how well you're doing on test day. Students are helped in identifying their areas of weakness by these. • Legal and regulatory framework implementation instructions that aid learners in both understanding the subject and putting it into practice as necessary. Following the generation of these outputs, material may be prepared and wrapped according to the specified style. With its many functions, the produced paper serves as an all-inclusive training and awareness handout. It has dual use: in simulated and real-world settings, for education and training purposes. This will aid in the definition of the procedure for quickly responding to potential security risks when necessary and in the complete learning of the security controls by both academic learners and the security operation teams. Sec. E. The Use of AI. The aforementioned learner parameters, in conjunction with the chosen course or security control, are parsed by the AI integration module. The Open AI API receives the prompt once it has been generated from the two structured datasets. By integrating with Open AI 4.0 via the Integration REST module, the newly built module may produce the pre-defined fields for training materials automatically. Table 1 displays the parameters that are used while interacting with the API. Afterwards, the output is reformatted in order to create a workbook including all of the required training materials.

TABLE I. OPEN AI API PARAMETERS

OPEN AI API Parameters	
Parameter	***Value***
API Model	GPT-4
Max Tokens	1500
Temperature	0.5-1.0

The built module is run and the results are checked. The prompt structure was revised many times to guarantee the most effective development of course materials and awareness guidelines. The most effective production of policies and their user-friendly instructions was guaranteed by improving the prompt. The findings were generated using the two datasets that were supplied. Both the list and the produced content were reviewed for quality. To guarantee that all potential risks associated with AI are addressed and controlled, the whole approach was improved within the parameters of the NIST AI RMF framework. Part F: Showing Off. The suggested module is put to the test by creating simulated learner profiles, material for various cyber security courses, and controls like NIST 800-171 and the ISO 27001/27002 set of controls. For the purpose of generating structured material for various controls, the shown content was sent to GPT-4, the most sophisticated API offered by OpenAI. All necessary materials were produced. G. Outcomes. Upon parsing the learner's profile and requested parameters using the AI API, a checklist of the choices the learner selected was created, along with the following content: · An overview of the training materials. o Basic Principles. o Intermediate and Advanced Topics. Competencies and Methods. o Slants on Criticism. on What's to Come in the Coming Years. materials and resources that are supplemental. • Step-by-step instructions for preliminary setup or task requirements. o Comprehensive Methods for Realization. things to think about or to be careful about. the Goal at the Conclusion. Security-Aware Coding: o Analysis Settings. o Configuring Virtual

Machines (VMs). We need scripts. to a deck of flash cards o Experiential Labs To evaluate: Applications in Real Life. o Practice for the Certificate Exam Objective Multiple-Choice Questions a Physical challenges Afterwards, the material is structured to create a whole instructional cycle, which is very effective for both standalone students and larger security operation teams. IV. FINAL Thoughts Security training, policies, and procedures are areas where organizations are investing significant resources; nonetheless, these areas may become vulnerable if not crafted properly. AI has shown to be a useful tool for creating these trainings and programs [13]. This content is kept up to date and to high standards by frequently revising it and bringing it into harmony with the latest released frameworks.

In this work, a method is defined for generating cyber security awareness and training utilizing artificial intelligence (AI) via created APIs. The mechanism is based on the capabilities of learners and the amount of achievement that is necessary. After some tweaks and analysis, the produced outputs proved to be both accurate and quite effective.

V. WHAT TO DO NEXT Cyber security students now have a vital resource in the form of regularly updated information that they may use to develop training and awareness materials specific to their needs and profiles. Like any other area of study in education, this one may be refined to provide further assurances of high-quality output.

REFERENCES

[1]. M. E. Erendor and M. Yildirim, "Cybersecurity Awareness in Online Education: A Case Study Analysis," in IEEE Access, vol. 10, pp. 52319 52335, 2022, doi: 10.1109/ACCESS.2022.3171829.

[2]. R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, ‘‘The impact of information richness on information security awareness training effectiveness,’’ Comput. Educ., vol. 52, no. 1, pp. 92–100, Jan. 2009.

[3]. A. Garba, M. Siraj, S. Othman, and M. Musa, ‘‘A study on cybersecurity awareness among students in Yobe State University, Nigeria: A quantitative approach,’’ Int. J. Emerg. Technol., vol. 11, no. 5, pp. 41–49, 2020.

[4]. V. Sundararajan, A. Ghodousi and J. E. Dietz, "The Most Common Control Deficiencies in CMMC non-compliant DoD contractors," 2022 IEEE International Symposium on Technologies for Homeland Security (HST), Boston, MA, USA, 2022, pp. 1-7, doi: 10.1109/HST56032.2022.10025445.

[5]. P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), Durgapur, India, 2020, pp. 1-3, doi: 10.1109/NCETSTEA48365.2020.9119914.

[6]. G. Langner, J. Andriessen, G. Quirchmayr, S. Furnell, V. Scarano and T. J. Tokola, "Poster: The Need for a Collaborative Approach to Cyber Security Education," 2021 IEEE European Symposium on Security and Privacy (EuroS&P), Vienna, Austria, 2021, pp. 719-721, doi: 10.1109/EuroSP51992.2021.00058.

[7]. M. Neumann, M. Rauschenberger and E. -M. Schön, "“We Need to Talk About ChatGPT”: The Future of AI and Higher Education," 2023 IEEE/ACM 5th International Workshop on Software Engineering Education for the Next Generation (SEENG), Melbourne, Australia, 2023, pp. 29-32, doi: 10.1109/SEENG59157.2023.00010.

[8]. Cisco Systems. (2008b). Data leakage worldwide: The effectiveness of corporate security policies. Retrieved May 12, 2011, from World Wide Web: http://www.cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/Cis co-STL-Data-Leakage-2008-.pdf

[9]. L. Li, W. He, L. Xu, A. Ivan, M. Anwar and X. Yuan, "Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study," 2014 Enterprise Systems Conference, Shanghai, China, 2014, pp. 169-173, doi: 10.1109/ES.2014.66.

[10]. National Institute of Standards and Technology. "AI Risk Management Framework." NIST January 26, 2023. Available online: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

[11]. J. C. Haass, "Cyber Threat

Intelligence and Machine Learning," 2022 Fourth International Conference on Transdisciplinary AI (TransAI), USA, 2022, pp. 156-159, doi: 10.1109/TransAI54797.2022.00033.

[12]. A. Martin-Lopez, "AI-Driven Web API Testing," 2020 IEEE/ACM 42nd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), Seoul, Korea (South), 2020, pp. 202 205.

[13]. W. Matsuda, M. Fujimoto, T. Aoyama and T. Mitsunaga, "Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud," 2019 IEEE Conference on Application, Information and Network Security (AINS), Pulau Pinang, Malaysia, 2019, pp. 54-59, doi: 10.1109/AINS47559.2019.8968698.

[14]. V. V. Ravi Kumar and R. Raman, "Student Perceptions on Artificial Intelligence (AI) in higher education," 2022 IEEE Integrated STEM Education Conference (ISEC), Princeton, NJ, USA, 2022, pp. 450-454, doi: 10.1109/ISEC54952.2022.10025165.

[15]. I. Ellefsen, "The development of a cyber security policy in developing regions and the impact on stakeholders," 2014 IST-Africa Conference Proceedings, Pointe aux Piments, Mauritius, 2014, pp. 1-10, doi: 10.1109/ISTAFRICA.2014.6880605.

[16]. R. Mishina, S. Tanimoto, H. Goromaru, H. Sato and A. Kanai, "Risk Management of Silent Cyber Risks in Consideration of Emerging Risks," 2021 10th International Congress on Advanced Applied Informatics (IIAI-AAI), Niigata, Japan, 2021, pp. 710-716, doi: 10.1109/IIAI AAI53430.2021.00126.

[17]. S. Tjoa, P. K. M. Temper, M. Temper, J. Zanol, M. Wagner and A. Holzinger, "AIRMan: An Artificial Intelligence (AI) Risk Management System," 2022 International Conference on Advanced Enterprise Information System (AEIS), London, United Kingdom, 2022, pp. 72-81, doi: 10.1109/AEIS59450.2022.00017.

[18]. M. T. Siponen, "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods", Information and organization, 15, 4, 2005, 339-375 [19] M. Warner, "Notes on the Evolution of Computer Security Policy in the US Government, 1965-2003," in IEEE Annals of the History of Computing, vol. 37, no. 2, pp. 8-18, Apr.-June 2015, doi: 10.1109/MAHC.2015.25.